1. (Original) A method comprising:

receiving a request to transfer application data from a source computing device to a destination computing device;

checking whether the application data can be transferred to the destination computing device, and if so, then checking whether the application data can be transferred under control of the user or a third party; and

receiving input from the appropriate one of the user or third party to control transferring of the application data to the destination computing device.

2. (Original) A method as recited in claim 1, further comprising:

checking whether the destination computing device is trusted to receive the application data; and

preventing the application data from being transferred if the destination computing device is not trusted to receive the application data.

3. (Original) A method as recited in claim 2, wherein checking whether the destination computing device is trusted to receive the application data comprises checking whether software executing on the destination computing device is trusted to receive the application data.

4. (Original) A method as recited in claim 2, wherein checking whether the destination computing device is trusted to receive the application data comprises the third party checking whether the destination computing device is trusted to receive the application data.

5. (Original) A method as recited in claim 2, wherein checking whether the destination computing device is trusted to receive the application data comprises having another party check, on behalf of the source computing device, whether the destination computing device is trusted to receive the application data.

6. (Original) A method as recited in claim 1, wherein checking whether the application data can be transferred comprises checking whether the application data is non-migrateable, user-migrateable, or third party-migrateable.

7. (Original) A method as recited in claim 6, further comprising:

if the application data is non-migrateable, then not allowing the application secret to be transferred;

if the application data is user-migrateable, then allowing the application secret to be transferred under control of a user; and

if the application data is third party-migrateable, then allowing the application secret to be transferred under control of a third party.

8. (Original) A method as recited in claim 6, wherein, if the application data is user-migrateable, then:

receiving input from the appropriate one of the user or third party comprises identifying a user passphrase;

the method further comprising:

identifying an encryption key previously used to encrypt the application data, wherein the encryption key corresponds to user-migrateable data,

encrypting the encryption key based at least in part on the user passphrase, and

allowing the encrypted encryption key to be copied to the destination computing device.

9. (Original) A method as recited in claim 6, wherein, if the application data is third party-migrateable, then:

receiving input from the appropriate one of the user or third party comprises identifying a public key of a public-private key pair associated with the third party;

the method further comprising:

identifying an encryption key previously used to encrypt the application secret, wherein the encryption key corresponds to third party-migrateable data,

encrypting the encryption key based at least in part on the public key, and

allowing the encrypted encryption key to be copied to the destination computing device.

10. (Original) A method as recited in claim 1, further comprising:

receiving application data to be encrypted and stored on the source computing device;

identifying how the application data is to be allowed to be transferred to the destination computing device if a request to transfer the application data is received; and

selecting a particular one of a plurality of encryption keys to encrypt the application data, wherein the selecting is based at least in part on how the application data is to be allowed to be transferred to another computing device.

11. (Original) A method as recited in claim 1, further comprising:

allowing application data for a plurality of applications to be transferred to the destination computing device by moving a single key to the destination computing device.

12-19. (Canceled).

20. (Original) One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a source computing device, causes the one or more processors to:

receive a request to transfer an application secret from the source computing device to a destination computing device;

identify a type of the application secret;

if the type is non-migrateable, then not allow the application secret to be transferred;

if the type is user-migrateable, then allow the application secret to be transferred under control of a user; and

if the type is third party-migrateable, then allow the application secret to be transferred under control of a third party.

21. (Original) One or more computer readable media as recited in claim 20, wherein the plurality of instructions to allow the application secret to be transferred under control of the user comprises a plurality of instructions to:

identify a user passphrase;

identify an encryption key previously used to encrypt the application secret, wherein the encryption key corresponds to the user-migrateable type;

encrypt the encryption key based at least in part on the user passphrase; and

allow the encrypted encryption key to be copied to the destination computing device.

22. (Original) One or more computer readable media as recited in claim 21, wherein the plurality of instructions to identify the user passphrase comprises a plurality of instructions to:

query the user for the passphrase; and

identify, as the passphrase, an input from the user in response to the query.

23. (Original) One or more computer readable media as recited in claim 20, wherein the plurality of instructions to allow the application secret to be transferred under control of the third party comprises a plurality of instructions to:

identify a public key of a public-private key pair associated with the third party;

identify an encryption key previously used to encrypt the application secret, wherein the encryption key corresponds to the third party-migrateable type;

encrypt the encryption key based at least in part on the public key; and

allow the encrypted encryption key to be copied to the destination computing device.

24. (Original) One or more computer readable media as recited in claim 20, wherein the plurality of instructions further cause the one or more processors to:

receive, from another computing device, a plurality of additional application secrets, wherein each of the additional application secrets is encrypted;

identify a first group of the plurality of additional application secrets that are to be decrypted under user control;

obtain, from the user, a passphrase; and

use the passphrase to decrypt each encrypted application secret of the first group.

25. (Original) One or more computer readable media as recited in claim 24, wherein the plurality of instructions further cause the one or more processors to:

identify a second group of the plurality of additional application secrets that are to be decrypted under third party control; and

communicate with a third party to have each encrypted application secret of the second group decrypted.

26. (Original) One or more computer readable media as recited in claim 20, wherein the third party comprises a smartcard.

27. (Original) One or more computer readable media as recited in claim 20, wherein the plurality of instructions further cause the one or more processors to:

authenticate the destination computing device as being trusted to receive the application secret; and

preventing the application secret from being transferred if the destination computing device is not trusted to receive the application secret.

28. (Original) One or more computer readable media as recited in claim 20, wherein the plurality of instructions further comprise instructions that cause the one or more processors to:

allow a plurality of application secrets to be transferred under control of the user by using a single key associated with the user-migrateable type.

29. (Original) One or more computer readable media as recited in claim 20, wherein the plurality of instructions further comprise instructions that cause the one or more processors to:

allow a plurality of application secrets to be transferred under control of the third party by using a single key associated with the third party-migrateable type.

30-40. (Canceled).

41. (Original) One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a computing device, causes the one or more processors to:

receive a plurality of encrypted application secrets from another computing device;

identify a first group of the plurality of encrypted application secrets that are to be decrypted under user control;

obtain, from a user, a passphrase;

use the passphrase to decrypt each encrypted application secret of the first group of encrypted application secrets;

identify a second group of the plurality of encrypted application secrets that are to be decrypted under third party control; and

communicate with a third party to have each encrypted application secret of the second group of encrypted application secrets decrypted.

42. (Original) One or more computer readable media as recited in claim 41, wherein each encrypted application secret of the first group comprises a user-migrateable application secret, and wherein each encrypted application secret of the second group comprises a third party-migrateable application secret.

43-48. (Canceled).

49. (Original) A method comprising:

receiving a request to transfer a plurality of application secrets from a source computing device to a destination computing device;

identifying which one of a plurality of types of application secrets the plurality of application secrets correspond to;

identifying a key associated with the one type;

allowing the plurality of application secrets to be accessible to the destination computing device by communicating the key to the destination computing device.

50. (Original) A method as recited in claim 49, wherein the type of application secret is all secrets and the key associated with the one type is a gatekeeper storage key.

51. (Original) A method as recited in claim 49, wherein the key comprises a hive key.

52. (Previously presented) A method comprising:

receiving a request to transfer data from a source computing device to a destination computing device;

checking whether the data can be transferred to the destination computing device, and if so, then checking whether the data can be transferred under control of the user or a third party; and

receiving input from the appropriate one of the user or third party to control transferring of the data to the destination computing device.

53. (Previously presented) A method as recited in claim 52, further comprising:

checking whether the destination computing device is trusted to receive the data; and

preventing the data from being transferred if the destination computing device is not trusted to receive the data.

54. (Previously presented) A method as recited in claim 52, wherein checking whether the data can be transferred comprises checking whether the data is non-migrateable, user-migrateable, or third party-migrateable.

55. (Previously presented) A method as recited in claim 54, further comprising:

if the data is non-migrateable, then not allowing the data to be transferred;

if the data is user-migrateable, then allowing the data to be transferred under control of a user; and

if the data is third party-migrateable, then allowing the data to be transferred under control of a third party.

56. (Previously presented) A method as recited in claim 52, further comprising:

allowing data for a plurality of applications to be transferred to the destination computing device by moving a single key to the destination computing device.

57. (Previously presented) A method as recited in claim 52, wherein the data comprises an operating system secret.

58. (Previously presented) A method as recited in claim 52, wherein the data comprises a trusted core secret.

59. (Previously presented) One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a source computing device, causes the one or more processors to:

receive a request to transfer data from the source computing device to a destination computing device;

identify a type of the data;

if the type is non-migrateable, then not allow the data to be transferred;

if the type is user-migrateable, then allow the data to be transferred under control of a user; and

if the type is third party-migrateable, then allow the data to be transferred under control of a third party.

60. (Previously presented) One or more computer readable media as recited in claim 59, wherein the plurality of instructions to allow the data to be transferred under control of the user comprises a plurality of instructions to:

encrypt an encryption key previously used to encrypt the data; and

allow the encrypted encryption key to be copied to the destination computing device.

61. (Previously presented) One or more computer readable media as recited in claim 59, wherein the plurality of instructions to allow the data to be transferred under control of the user comprises a plurality of instructions to:

identify a user passphrase;

identify an encryption key previously used to encrypt the data, wherein the encryption key corresponds to the user-migrateable type;

encrypt the encryption key based at least in part on the user passphrase; and

allow the encrypted encryption key to be copied to the destination computing device.

62. (Previously presented) One or more computer readable media as recited in claim 59, wherein the plurality of instructions to allow the data to be transferred under control of the third party comprises a plurality of instructions to:

encrypt an encryption key previously used to encrypt the data; and

allow the encrypted encryption key to be copied to the destination computing device.

63. (Previously presented) One or more computer readable media as recited in claim 59, wherein the plurality of instructions to allow the data to be transferred under control of the third party comprises a plurality of instructions to:

identify a public key of a public-private key pair associated with the third party;

identify an encryption key previously used to encrypt the data, wherein the encryption key corresponds to the third party-migrateable type;

encrypt the encryption key based at least in part on the public key; and

allow the encrypted encryption key to be copied to the destination computing device.

64. (Previously presented) One or more computer readable media as recited in claim 59, wherein the plurality of instructions further cause the one or more processors to:

authenticate the destination computing device as being trusted to receive the data; and

preventing the data from being transferred if the destination computing device is not trusted to receive the data.

65. (Previously presented) One or more computer readable media as recited in claim 59, wherein the plurality of instructions further comprise instructions that cause the one or more processors to:

allow multiple data to be transferred under control of the user by using a single key associated with the user-migrateable type.

66. (Previously presented) One or more computer readable media as recited in claim 59, wherein the data comprises an operating system secret.

67. (Previously presented) One or more computer readable media as recited in claim 59, wherein the data comprises a trusted core secret.

68-75. (Canceled).

76. (Previously presented) A method comprising:

receiving a request to transfer a plurality of secrets from a source computing device to a destination computing device;

identifying which one of a plurality of types of secrets the plurality of secrets correspond to;

identifying a key associated with the one type; and

allowing the plurality of secrets to be accessible to the destination computing device by communicating the key to the destination computing device.

77. (Previously presented) A method as recited in claim 76, wherein the type of secret is all secrets and the key associated with the one type is a gatekeeper storage key.

78. (Previously presented) A method as recited in claim 76, wherein the plurality of secrets comprises one or more operating system secrets.

79. (Previously presented) A method as recited in claim 76, wherein the plurality of secrets comprises one or more trusted core secrets.